DEPARTMENT OF FINANCE BILL ANALYSIS

AMENDMENT DATE: June 20, 2011
POSITION: Neutral

BILL NUMBER: SB 24
AUTHOR: J. Simitian
RELATED BILLS: SB 1166, SB 20

BILL SUMMARY: Personal Information: Privacy

This bill amends current security breach notification law as specified in sections 1798.29 and 1798.82 of the Civil Code. These sections apply to state agencies, persons, or businesses conducting business in California that own or license computerized data that includes personal information. The bill has the following four components:

1. Specifies security breach notices be written in plain language and include certain standard information.
2. Requires notification to the Attorney General (AG) if more than 500 California residents are affected by a single breach.
3. Requires notification to either the Office of Information Security (OIS) within the California Technology Agency (Technology Agency), or the Office of Privacy Protection (OPP) within the State and Consumer Services Agency, if the substitute notice provision in current law is used as notification. (OIS is notified if the entity experiencing the breach is an agency; OPP is notified if the entity experiencing the breach is a person or business conducting business in California.) Substitute notice consists of e-mail, Internet website posting, and notifying major statewide media. Substitute notice is permitted if the costs would exceed $250,000; the number of persons exceeds 500,000; or if the agency does not have sufficient contact information.
4. Specifies that a covered entity under the federal Health Insurance Portability and Accountability Act of 1996 (HIPAA) is deemed compliant with the provisions of this bill if it has complied with the federal Health Information Technology for Economic and Clinical Health (HITECH) Act. The HITECH Act requires notification to patients whose health information has been breached, and specifies certain items to be included in the notification, such as the date of the breach and the types of information involved.

This bill is almost identical to SB 1166 of 2010 and SB 20 of 2009, both of which were vetoed by former Governor Schwarzenegger with the same veto message. The veto message maintained that these bills were unnecessary because there is no evidence that there is a problem with the information currently provided to consumers, and that no additional consumer benefit is gained by requiring the AG to receive breach notices as the AG is not required to do anything with them.

FISCAL SUMMARY

Specified Content for Security Breach Notifications

- Fiscal impact to state agencies is most likely extremely minor, if any. According to the author's staff, SB 24 is primarily directed at the private sector.

Notification to the Attorney General

The AG has not yet completed their analysis of SB 24, but indicated that they do not expect to experience a significant programmatic or fiscal impact as the AG has been receiving notifications of breaches from businesses and is prepared to receive and handle additional notifications.

Analyst/Principal	Date	Program Budget Manager	Date
(0821) S. Davis-James		Diana Ducay	

Department Deputy Director Date

Governor's Office: By: Date: Position Approved_____
Position Disapproved_____

Notification to the OIS and the OPP
The Technology Agency, which houses the OIS, indicated that this bill would create "only minor and absorbable costs." The OPP indicated previously in regards to SB 1166 that the bill would have a minimal fiscal impact. Existing policy in section 5350.1 of the State Administrative Manual already requires state agencies to report security breaches to the OIS regardless of whether they resulted in a breach notification. The Technology Agency has taken a neutral position on this bill as they are already largely compliant with its requirements.

COMMENTS

The following stakeholders and interested parties have expressed support for SB 24:

- Privacy Activism, Privacy Rights Clearinghouse, California Schools Employee Association, California State Sheriffs Association, California Association of Health Underwriters, American Civil Liberties Union.

The Senate bill analysis provides additional information regarding similar legislation in other states and clarifies how SB 24 aligns with federal regulations:

- Other states: Fourteen states, including Hawaii, Virginia, North Carolina, Iowa, and Michigan, have passed similar legislation for security breach notifications using existing California law as a model, as well as including many of the requirements proposed in SB 24.
- Federal law: SB 24 aligns with the HITECH Act, which applies to HIPAA-covered entities, and contains some additional requirements over and above the Act.

General Comments
- It appears this bill would enhance the content of breach notifications which are already required to be issued in the event of a security breach. The Senator's staff indicated that breach notifications they had seen from the private sector tended to be lacking in detail and unclear, compared to notifications issued by government offices.
- There will most likely be minimal fiscal and operational impact on state agencies or persons/businesses conducting business in California.
- We note that a state agency can be a HIPAA-covered entity; however the reference to HIPAA-covered entities is only included in Civil Code section 1798.82, which applies to persons or businesses conducting business in California, not agencies.

Code/Department Agency or Revenue Type	SO LA CO RV	(Fiscal Impact by Fiscal Year) (Dollars in Thousands) PROP 98	FC	2011-2012	FC	2012-2013	FC	2013-2014	Fund Code
0820/Justice	SO	No		---------- No/Minor Fiscal Impact ----------					0001
0502/Tech Agency	SO	No		---------- No/Minor Fiscal Impact ----------					0001
0510/Secty SCS	SO	No		---------- No/Minor Fiscal Impact ----------					0001